ABSTRACT

As shown in Fig. 2, when the SYN segment is detected, the amount of transmitted segment from the side which sent the detected SYN segment is obtained by counting the continuously detected DATA segments for collecting the traffic in a certain direction where it is impossible to directly capture the traffic. Further, the amount [ini __sdt] of the transmitted bytes from the side which sent the detected SYN segment is obtained by calculating the equation [ini__sdt]=[SEQn+LENn]-[SEQ1]. Wherein, [SEQ1] is the sequence number of the first detected DATA segment, [SEQn] is the sequence number of the last detected DATA segment and [LENn] is the user data length of the last detected DATA segment.